Samsung Community / Products / ‹ Computers & IT
/ **Samsung SSD 970 EVO Plus drive encryption won't change from Ready to Enable**

Original topic:

Samsung SSD 970 EVO Plus drive encryption won't change from Ready to Enable

Topic Options ⋮

(Topic created on: 18-10-2019 09:00 AM) 30100 Views

Labels: Memory & Storage

- Close original thread and solution

QuitchApprentice

OPTIONS ⋮

18-10-2019 09:00 AM - last edited 18-10-2019 09:01 AM

I am setting up a brand new machine with the above drive and have installed a discrete TPM 2.0 header on the motherboard to allow me to use hardware encryption with BitLocker. Windows 10 Pro x64 1903 is in use.

I installed Windows and Samsung Magician 6.0 and switched on drive encryption within the Encrypted Drive part of the tool. It shows "Ready to Enable" as a status. I create the Secure Erase tool, but the tool cannot find the drive. Going back into Windows I updated the drive's firmware to 2B2QEXM7. I reboot and run Secure Erase. The drive is successfully detected and the tool reports that it completed successfully. On rebooting the computer cannot detect bootable media, indicating success.

I disable Legacy USB and CSM support in UEFI, then boot my Windows 10 USB installer. The drive is showing as empty, no partitions. I create a single disk partition (with Windows creating its standard recovery partitions) and finish the install.

After booting into Windows I install Samsung Magician, but Encrypted Drive is still reporting the drive as "Ready to Enable" rather than "Enabled". I try repeating the Secure Erase and installing Windows process, but the status is still "Ready to Enable".

I've done this previously (on a different computer) with a Samsung SS 840 EVO, but did not encounter this problem. At this point I am not sure what more I can do. It would seem that Secure Erase is not flipping whatever switch it is supposed to, but it's not reporting any errors and is erasing the drive. The Windows 10 install is on a completely fresh drive.

bitlocker | encrypted drive | Encryption | ready to enable | secure erase

2 Likes

REPLY

13 REPLIES

‹ Previous 1 2 Next ›

PaulNecsoiuFirst Poster

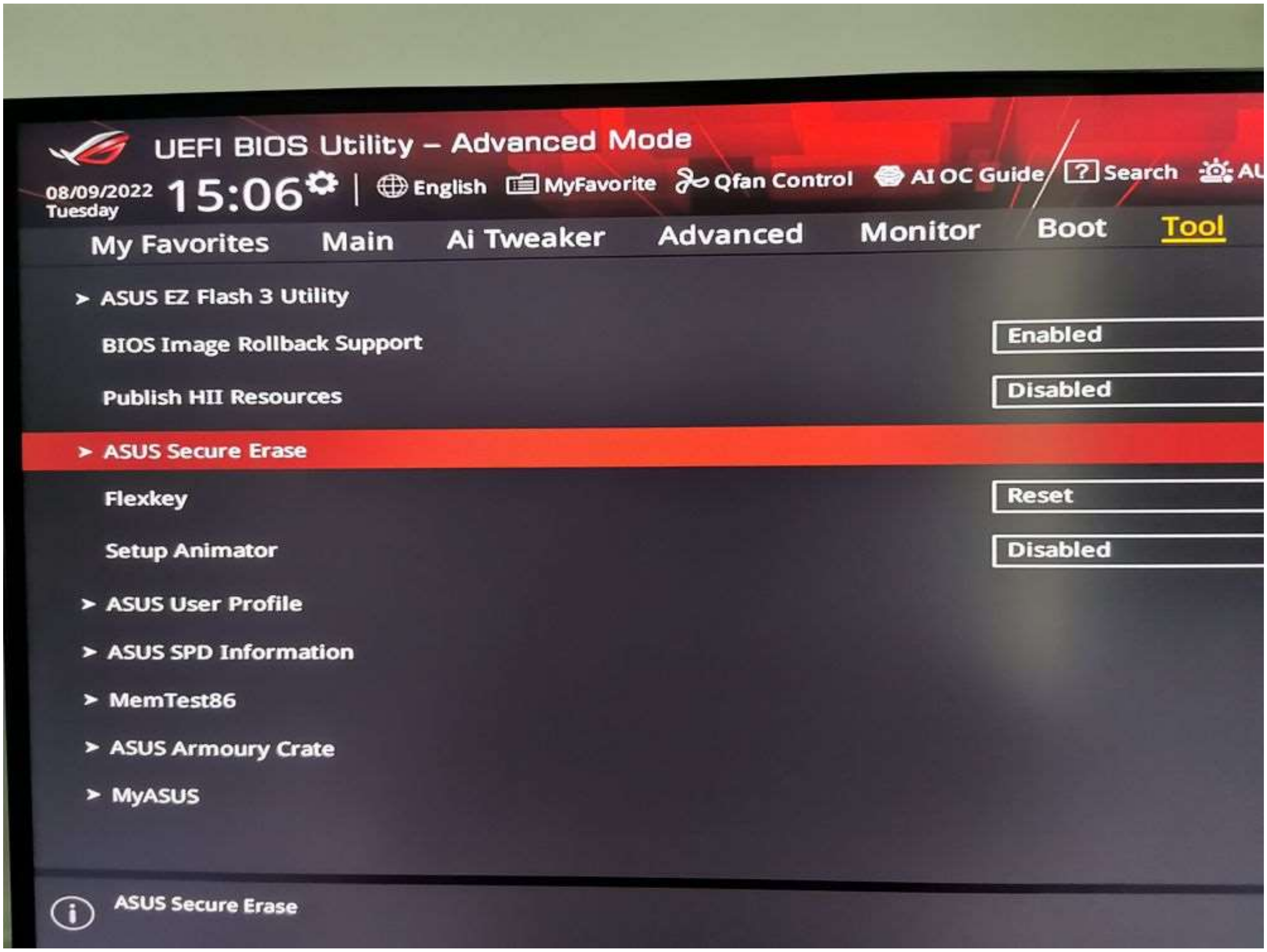
OPTIONS ⋮

09-08-2022 12:44 PM - last edited 09-08-2022 01:14 PM

After countless hours of testing and trying I will post the steps I took for a specific configuration, maybe it will help others.

Motherboard: ROG STRIX Z690-I GAMING WIFI Bios version: 1601
SSD: Samsung 980 Pro NVME Firmware version: 5B2QGXA7

Because the USB stick created with Magician (version 7.1.1) doesn't boot I have performed a Secure Erase using the motherboard BIOS Option (**Tools -> Asus Secure Erase**).



➤ ASUS EZ Flash 3 Utility

BIOS Image Rollback Support: Enabled

Publish HII Resources: Disabled

➤ ASUS Secure Erase

Flexkey: Reset

Setup Animator: Disabled

➤ ASUS User Profile

➤ ASUS SPD Information

➤ MemTest86

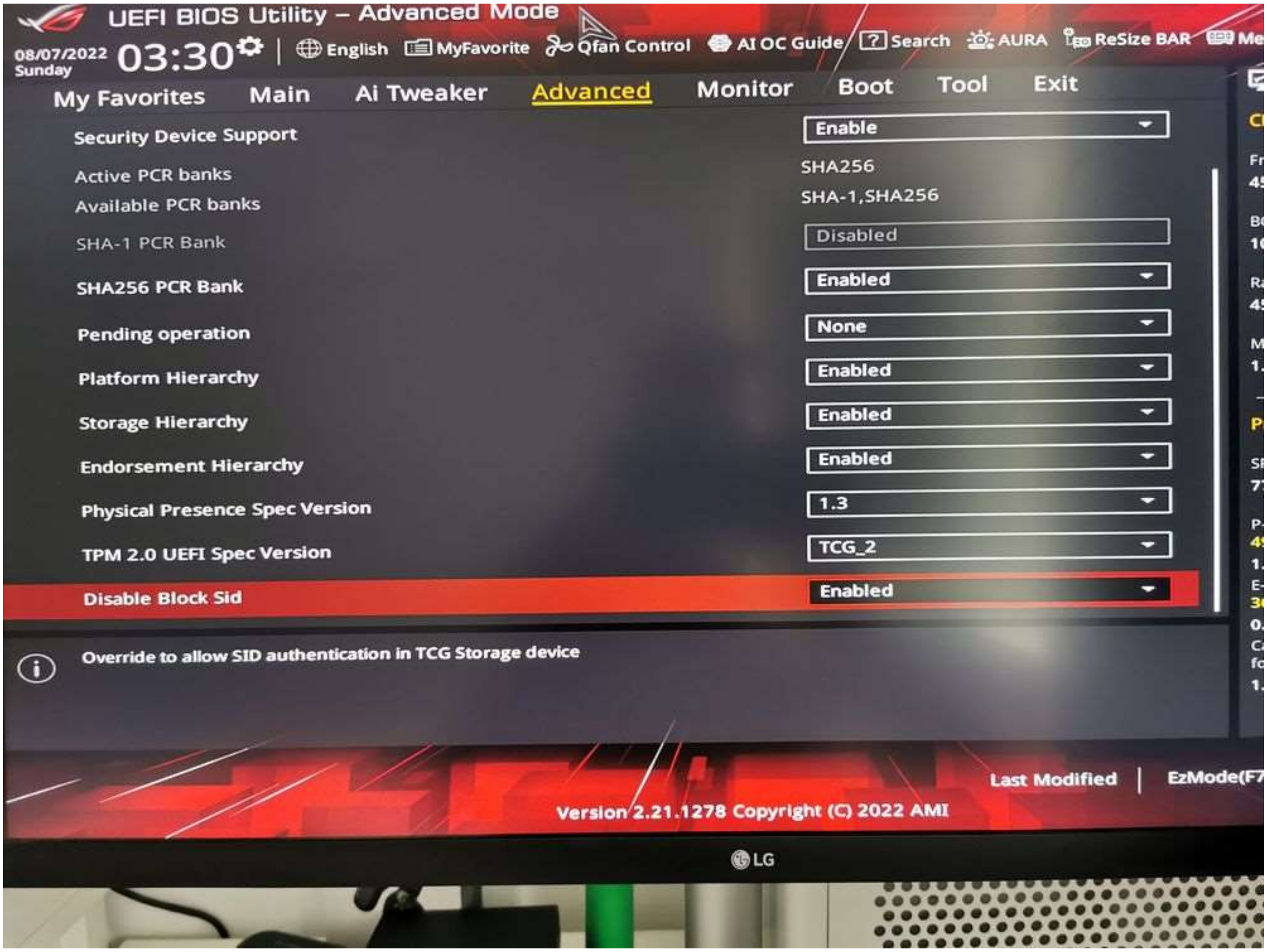
➤ ASUS Armoury Crate

➤ MyASUS

ⓘ ASUS Secure Erase

NOTE (as I have documented): Secure Erasing put the drive in factory state and generate a new DEK (encryption key) used to encrypt data on the drive. So, if you don't intend to generate a new key (and especially in the case of new drives) I don't think it is absolutely necessary to do a Secure Erase of the drive. (maybe someone with a new drive can confirm this).

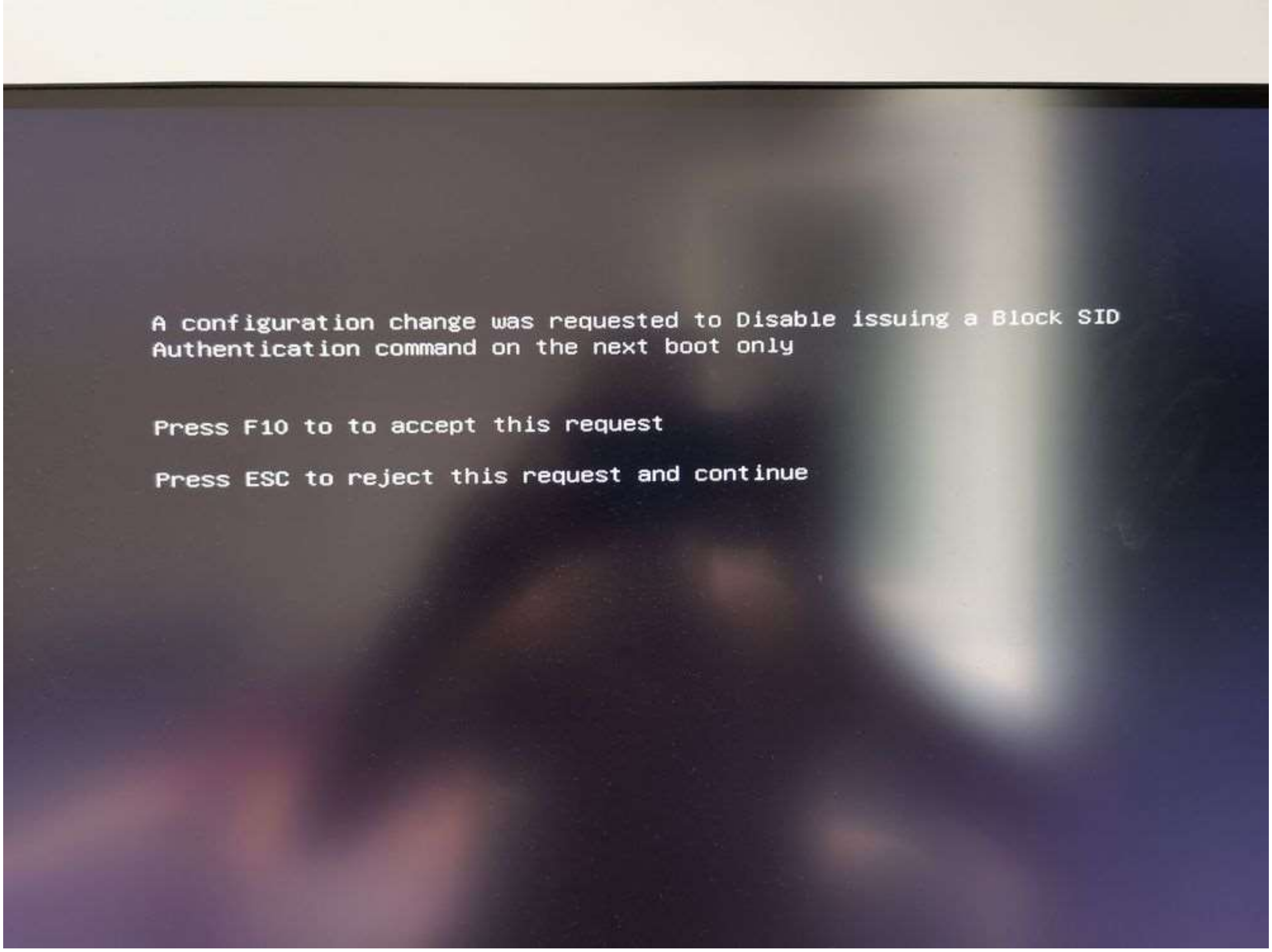
To Enable "Encrypted Drive", I had to temporary disable "Block SID". On my board it can be disabled only "for one boot" (meaning that after reboot the setting will toggle again to enabled), but it was enough.
Also note that on my BIOS the Option name is "**Disable Block Sid**" which means that in order to deactivate it, it must be set to the **Enable** state.



Security Device Support Enable
Active PCR banks SHA256
Available PCR banks SHA-1,SHA256
SHA-1 PCR Bank Disabled
SHA256 PCR Bank Enabled
Pending operation None
Platform Hierarchy Enabled
Storage Hierarchy Enabled
Endorsement Hierarchy Enabled
Physical Presence Spec Version 1.3
TPM 2.0 UEFI Spec Version TCG_2
Disable Block Sid Enabled

Override to allow SID authentication in TCG Storage device

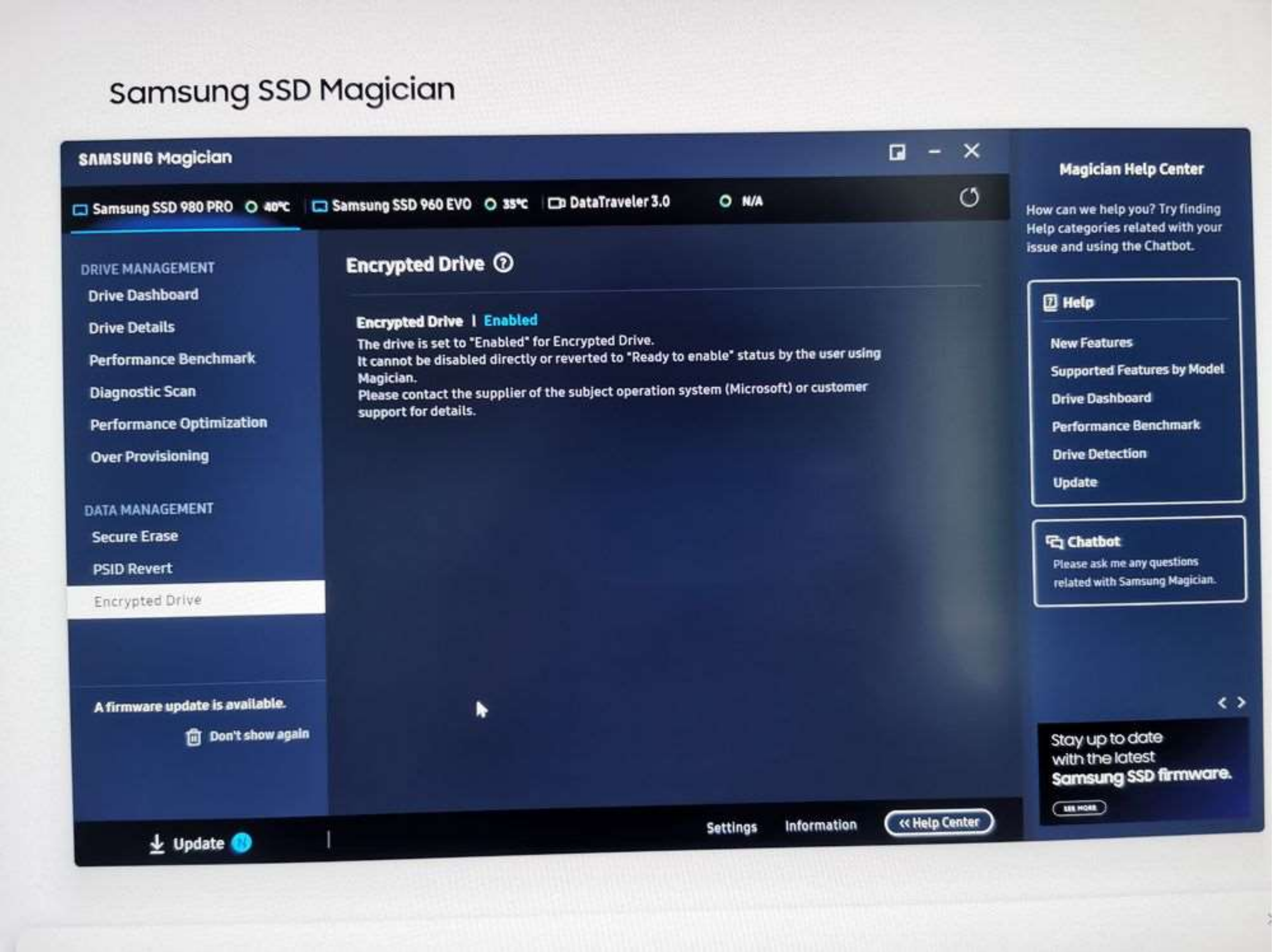
After Disabling Block SID I was presented with this screen:



```
A configuration change was requested to Disable issuing a Block SID
Authentication command on the next boot only

Press F10 to to accept this request

Press ESC to reject this request and continue
```

After that I have booted the Windows 11 installation media (Windows 11 bootable USB stick) and installed Windows 11.

After installation:



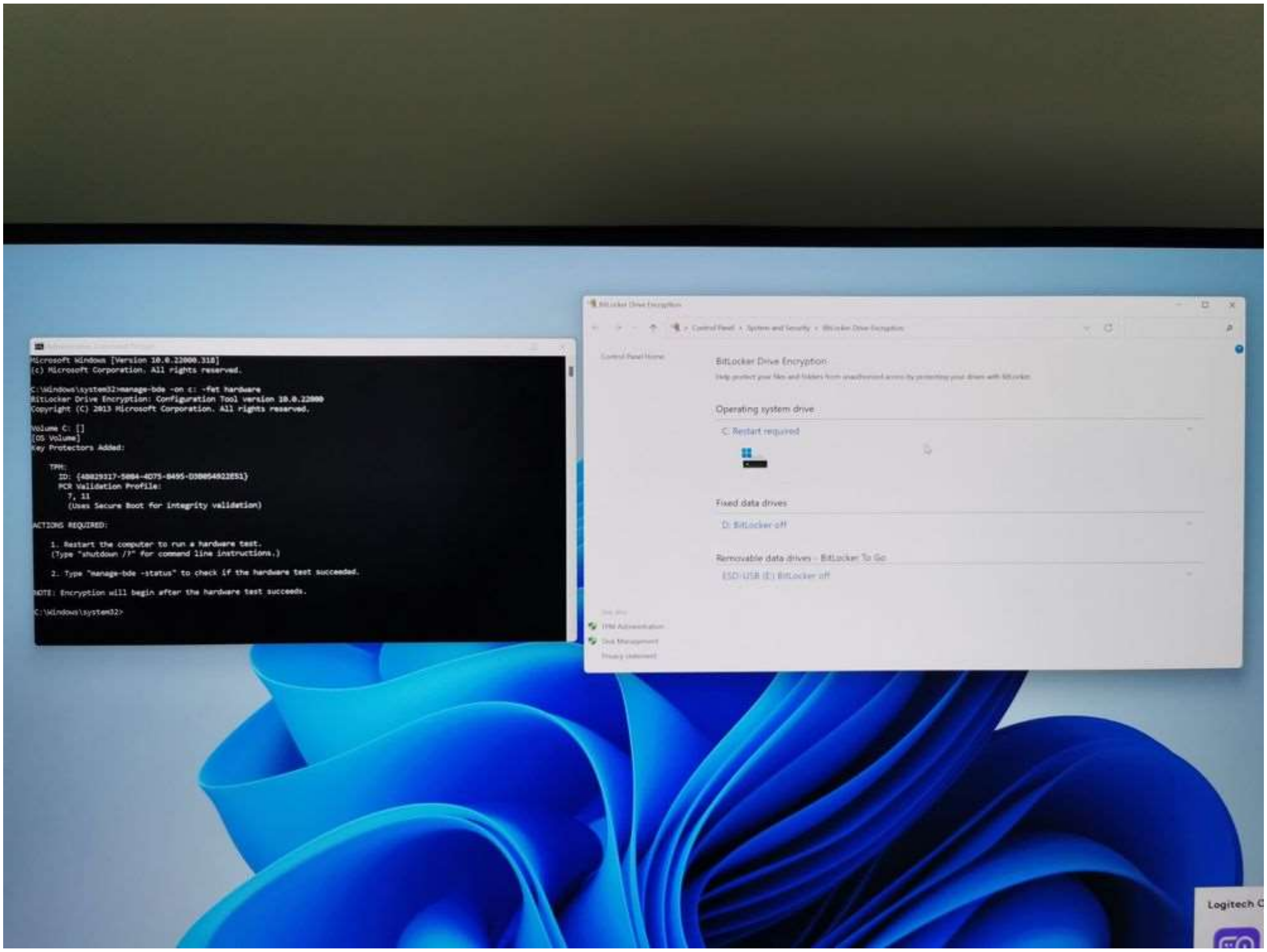
Encrypted Drive

Encrypted Drive | Enabled

The drive is set to "Enabled" for Encrypted Drive.
It cannot be disabled directly or reverted to "Ready to enable" status by the user using Magician.
Please contact the supplier of the subject operation system (Microsoft) or customer support for details.

Now you can use BitLocker to hardware encrypt your system volume, **BUT BE AWARE** that by default BitLocker uses software encryption.

So, in order to hardware encrypt your volume you need to use the BitLocker command-line tool (manage-bde) :
manage-bde –on C: -fet Hardware



```
Microsoft Windows [Version 10.0.22000.318]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -on c: -fet hardware
BitLocker Drive Encryption: Configuration Tool version 10.0.22000
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: []
[OS Volume]
Key Protectors Added:

    TPM:
      ID: {40829317-5084-4D75-8495-D38054922E51}
      PCR Validation Profile:
        7, 11
        (Uses Secure Boot for integrity validation)

ACTIONS REQUIRED:

    1. Restart the computer to run a hardware test.
    (Type "shutdown /?" for command line instructions.)

    2. Type "manage-bde -status" to check if the hardware test succeeded.

NOTE: Encryption will begin after the hardware test succeeds.

C:\Windows\system32>
```

BitLocker Drive Encryption

Control Panel > System and Security > BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: Restart required

Fixed data drives

D: BitLocker off

Removable data drives - BitLocker To Go

ESD-USB (E:) BitLocker off

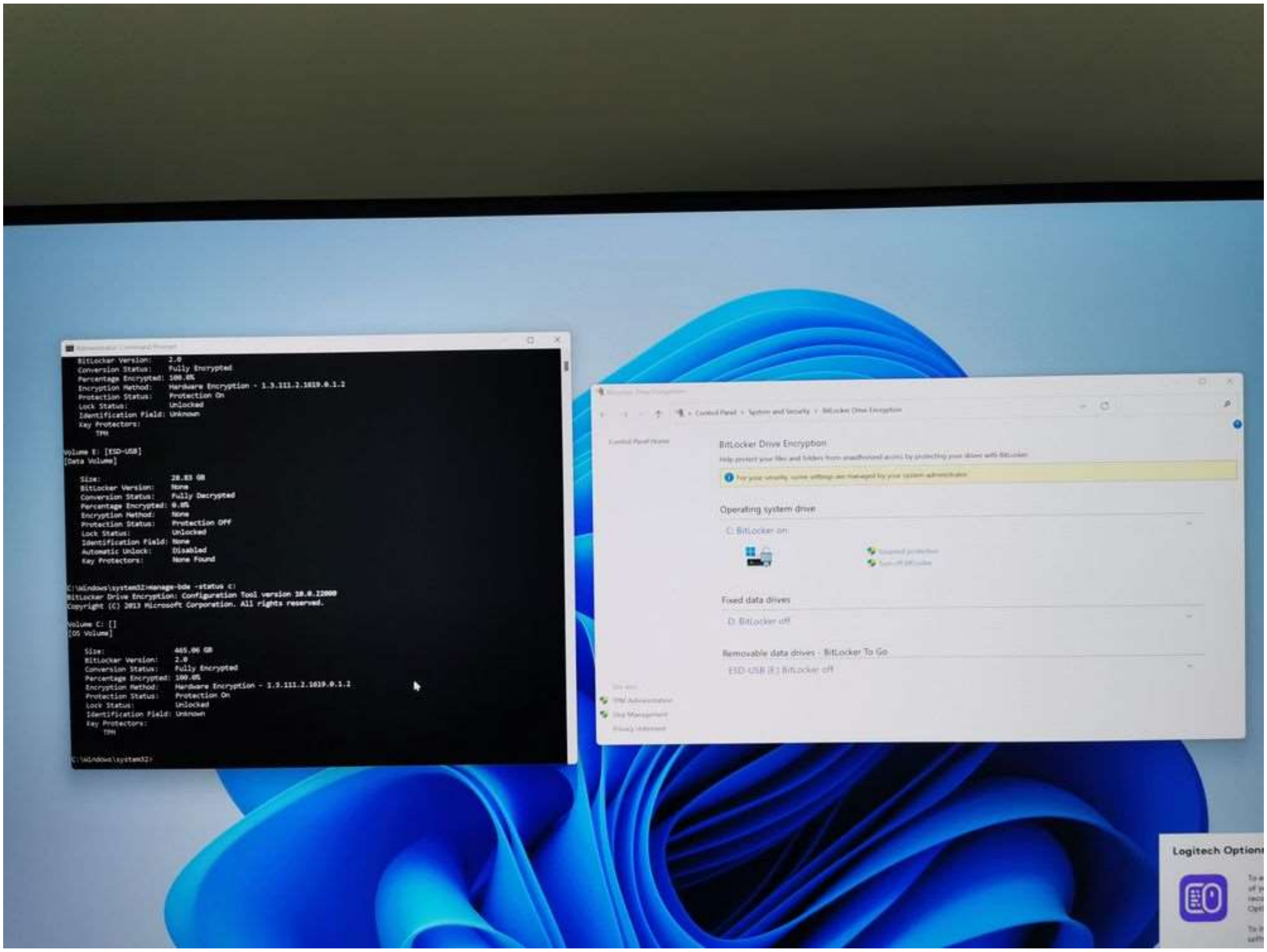
See also

TPM Administration

Disk Management

Privacy statement

After computer restart:

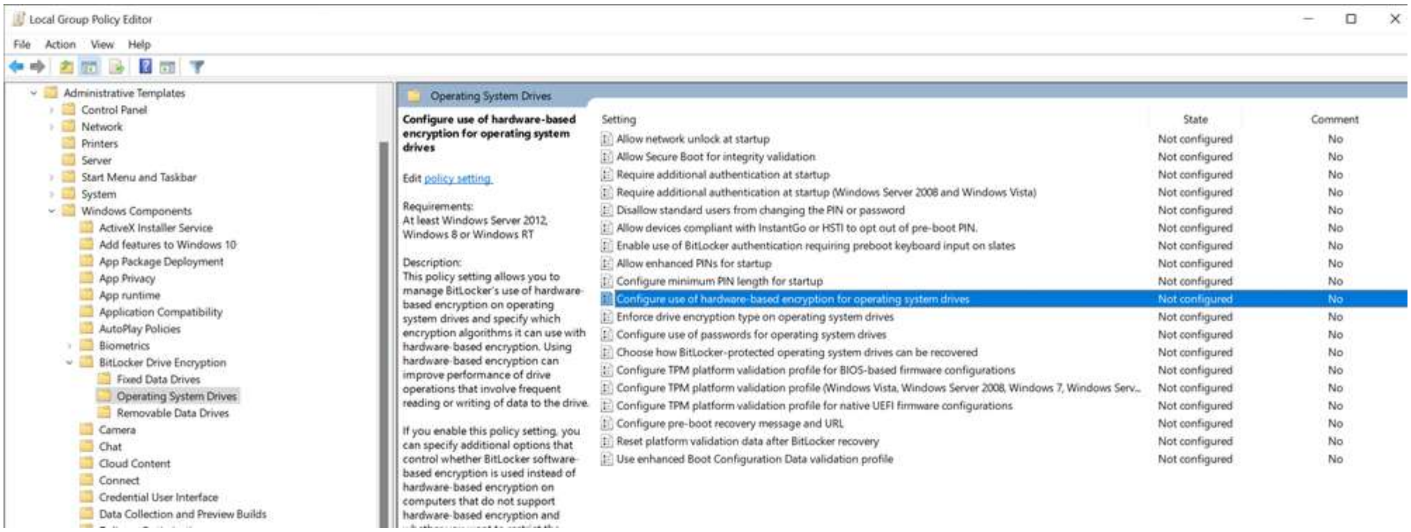


```
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    Hardware Encryption - 1.3.111.2.1619.0.1.2
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        TPM

Volume E: [ESD-USB]
[Data Volume]

    Size:                 28.83 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found

C:\Windows\system32>manage-bde -status c:
BitLocker Drive Encryption: Configuration Tool version 10.0.22000
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: []
[OS Volume]

    Size:                 465.06 GB
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    Hardware Encryption - 1.3.111.2.1619.0.1.2
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        TPM

C:\Windows\system32>
```

Control Panel > System and Security > BitLocker Drive Encryption
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker
For your security, some settings are managed by your system administrator
Operating system drive
C: BitLocker on
Suspend protection
Turn off BitLocker
Fixed data drives
D: BitLocker off
Removable data drives - BitLocker To Go
ESD-USB (E:) BitLocker off
See also
TPM Administration
Disk Management
Privacy statement
Logitech Options

If you want that BitLocker use by default hardware SED encryption then you need to use BitLocker group policy settings.

For example, for hardware encryption of the Operating System Drives (my case) you need to Enable "**Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives**"



Configure use of hardware-based encryption for operating system drives

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This policy setting allows you to manage BitLocker's use of hardware-based encryption on operating system drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive.

If you enable this policy setting, you can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No
Require additional authentication at startup (Windows Server 2008 and Windows Vista)	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN.	Not configured	No
Enable use of BitLocker authentication requiring preboot keyboard input on slates	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption for operating system drives	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives can be recovered	Not configured	No
Configure TPM platform validation profile for BIOS-based firmware configurations	Not configured	No
Configure TPM platform validation profile (Windows Vista, Windows Server 2008, Windows 7, Windows Serv...	Not configured	No
Configure TPM platform validation profile for native UEFI firmware configurations	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

1 Like REPLY

Tek4First Poster

OPTIONS ⋮

↳ In response to **PaulNecsoiu**

12-03-2023 08:43 AM in

Samsung Secure Erase ***CERTAINLY DOES BOOT***, but not in UEFI mode. You need to go to the BIOS Boot screen and enable CSM (Compatibility Support Module). In the Secure Boot screen, you need to specify "Other OS" (not "Windows UEFI Mode"). After running Secure Erase, you'll need to change these settings back in order to boot Windows.

1 Like REPLY

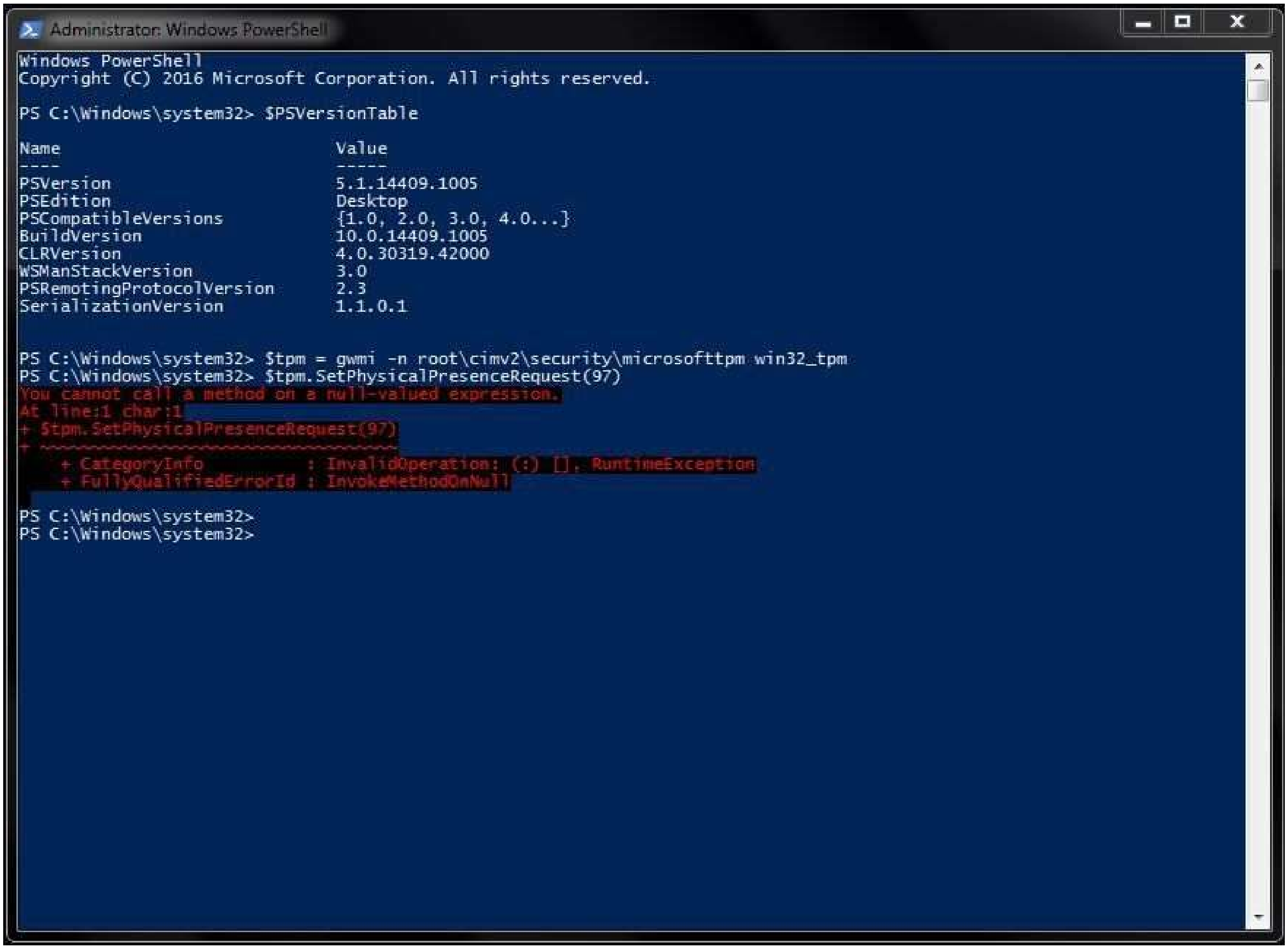
Mizu23xFirst Poster

OPTIONS ⋮

↳ In response to **denis795**

14-08-2023 11:37 PM in

Greetings!
I tried to follow your tutorial, but now i am stuck in powershell(as administrator)..



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.14409.1005
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.14409.1005
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1


PS C:\Windows\system32> $tpm = gwmi -n root\cimv2\security\microsofttpm win32_tpm
PS C:\Windows\system32> $tpm.SetPhysicalPresenceRequest(97)
You cannot call a method on a null-valued expression.
At line:1 char:1
+ $tpm.SetPhysicalPresenceRequest(97)
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : InvokeMethodOnNull

PS C:\Windows\system32>
PS C:\Windows\system32>
```

I have no idea how to use PowerShell and i don't have the option to disable "block sid" in my Uefi Bios on MB Z170 Pro gaming. I think this problem appear because i have windows 7 with an older PowerShell version (5.1), but i am not sure about that.

I want to use Bitlocker with hardware encryption on ssd m2 970 evo plus 1tb and I will install windows 10 pro on that 970 evo plus

Here is some system information:

OS Name Microsoft Windows 7 Ultimate x64
Version 6.1.7601 Service Pack 1 Build 7601
BIOS Version/Date American Megatrends Inc. 3805, 16.05.2018
Motherboard Z170 Pro gaming (with last bios update and last Intel ME update)

My problems..
1.How to disable "block sid"?

2.I heard that i need to disable "Legacy mode" - The computer must always boot natively from UEFI. If i disable (CSM) that mean the computer will run only on UEFI? CSM = legacy mode? i am not sure.

3.I want to use only a password for bitlocker, i mean i don't want the ssd to work only on my motherboard(i want to put it in other pc's). I think that mean i don't have to use tpm? is that possible? Thanks!

0 Likes

REPLY

denis795 Apprentice

OPTIONS ⋮

↳ In response to **Mizu23x**

21-08-2023 08:33 PM in

Hi,

Powershell version must be OK. Othervise i would expect error to be something like "does not contain a method SetPhysicalPresenceRequest" or "Class not exist". Maybe try to clear TPM from a bios and try again. If same error - then most likely Your MB/UEFI refuses to config this stuff via powershell.

Reg. legacy mode/CSM/UEFI -- from my experience at the end You need CSM=disabled / Legacy mode=disabled. Not sure though if You won't run into issues with this because of Windows 7. Not what i didn't like Windows 7, i did a lot beleive me. But it is like few years EOL, so good oportunity to update. Maybe it even would let You succeed with $tpm.SetPhysicalPresenceRequest(97) ..

Yes, You can do bitlocker without TPM, with password input on boot. You need to change option via gpedit.msc. Google - "GPO Bitlocker without TPM" - for instructions. Although, even if You go with TPM You will also receive long recovery string upon enabling. You can use that string to unlock drive on another pc. Or on the same pc if it's TPM get's cleared or breaks, or You make some big changes to hardware in Your PC. Just be cautious that it will not always work with Hardware Encryption, because that "other pc" might not be compatible with it. For example, if i pull out one of SATA3 Hardware Encrypted disks and try to connect it to other PC (or even to the same) via SATA-to-USB adapter - it won't ever work. Cause HW encryption requires SATA with AHCI mode, native MS drivers etc, etc. So in scenarious where You need to frequently move bitlocker-encrypted drive around PCs without much headache i would suggest using software encryption.

0 Likes

REPLY

‹ Previous 1 2 Next ›

Related Content

SSD 990 PRO: BitLocker encryption not working ›

in Computers & IT a month ago

Issues with the Samsung Odyssey G9 Neo and What I've tried to solve it! ›

in Computers & IT 06-05-2023

RAPID Mode on 850 EVO SSD problem ›

in Computers & IT 14-02-2023

Odyssey Neo G9 - connecting two devices (is a pain) ›

in Computers & IT 13-05-2022

Samsung Magician Secure Erase: Keyboard cannot be used ›

in Computers & IT 25-04-2022

Top tags ›

bitlocker Encryption Eye Saver mode monitor Samsung odysey g9 sj55w

SSD Ultra Wide warranty

Cookie Preferences

COOKIES TERMS AND CONDITIONS PRIVACY LEGAL UNITED KINGDOM / ENGLISH

Copyright© 1995-2024 All Rights Reserved.